REMARKS

This application has been carefully reviewed in light of the Office Action dated May 29, 2003. Claims 1 to 3, 6, 7, 10 to 14, 18 to 20 and 22 remain in the application, of which Claims 1, 10, 14, 18, 20 and 22, the independent claims herein, have been amended. Reconsideration and further examination are respectfully requested.

Claims 1, 3, 6, 10 and 12 to 14 were rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 5,619,025 (Hickman), Claims 2 and 11 were rejected under 35 U.S.C. § 103(a) over Hickman, and Claims 7, 18 to 20 and 22 were rejected under § 103(a) over Hickman in view of Schneier (Applied Cryptography). Reconsideration and withdrawal of the rejections are respectfully requested.

The present invention concerns encryption of digital information. According to the invention, an encryption key is obtained from an external source and stored in a storage means to execute an encryption process. The stored external encryption key is used to encrypt either digital information or an internal encryption key that has been used to encrypt the digital information. The encrypted digital information and the encrypted internal encryption key art then output. However, after completion of the encryption process using the stored external encryption key, and before the encrypted digital information and the encrypted internal encryption key are output, the stored external encryption key is erased from the storage means. As a result, the external encryption key is erased from the storage means sooner than in conventional systems, thereby significantly reducing the time that the key is stored and consequently reducing the time available for a hacker will be able to obtain the external encryption key from the storage means.

With specific reference to the claims, amended independent Claim 1 is an image input apparatus comprising reading means for reading an encryption key stored in an external source, storage means for storing the encryption key to execute an encryption process, encryption means for encrypting digital information by using the encryption key stored in the storage means, output means for outputting the encrypted digital information, and erasing means for erasing the encryption key stored in the storage means after encrypting the digital information by the encryption means and before outputting the encrypted digital information by the output means.

Amended independent Claims 10 and 14 are method and computer program claims, respectively, that substantially correspond to Claim 1.

Amended independent Claim 18 is an image input apparatus comprising information encryption means for encrypting digital information by using an internal encryption key, obtaining means for obtaining an external encryption key stored in an external source, storage means for storing the external encryption key to execute a key encryption process, key encryption means for encrypting the internal encryption key by using the external encryption key stored in the storage means, output means for outputting the encrypted digital information and the encrypted internal encryption key, and erasing means for erasing the external encryption key stored in the storage means after encrypting the internal encryption key by the key encryption means and before outputting the encrypted digital information and the encrypted internal encryption key by the output means.

Amended independent Claims 20 and 22 are method and computer program claims, respectively, that substantially correspond to Claim 18.

The applied art, alone or in combination, is not seen to disclose or to suggest the features of independent Claims 1, 10, 14, 18, 20 and 22. More particularly, the applied art is not seen to disclose or to suggest at least the feature of erasing an external encryption key stored in a storage means after encrypting digital information and/or an internal encryption key using the external encryption key and before outputting the encrypted digital information and/or the encrypted internal encryption key by an output means.

Hickman is merely seen to disclose a laser and crystal diode technique for verifying a document such as a credit card. At column 5, lines 7 to 12, Hickman discloses that the image data (the refractive characteristics of the crystals used on a magnetic stripe of a credit card) may be used as an encryption key. The encryption key may be used to transmit data to an electronic database. However, Hickman specifically states that "[a]fter a transmission is completed, the encryption key is erased immediately in the database bank, thus insuring internal security of data transmission." Therefore, Hickman, like many of the other art of record cited in previous Office Actions, only erases the encryption key *after* the transmission has been completed and does not erase the key after the encryption and before outputting the encrypted digital information. Accordingly, Hickman is not seen to disclose or to suggest the features of the present invention.

Schneier is not seen to add anything to overcome the deficiencies of Hickman and is also not seen to disclose or to suggest at least the feature of erasing an

external encryption key stored in a storage means after encrypting digital information and/or an internal encryption key using the external encryption key and before outputting the encrypted digital information and/or the encrypted internal encryption key by an output means.

In view of the foregoing amendments and remarks, the entire application is believed to be in condition for allowance and such action is respectfully requested at the Examiner's earliest convenience.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicant

Registration No. 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

CA_MAIN 68630 v 1